

UNITED STATES DISTRICT COURT

for the
Northern District of OklahomaIn the Matter of the Search of
[kayjohns145@gmail.com] THAT IS STORED AT THE
PREMISES CONTROLLED BY GOOGLE INC.

Case No. 20-mj-150-FHM

FILED
JUN 10 2020
Mark C. McCarthy, Clerk
U.S. DISTRICT COURT

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A"

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252(a)(2) and (b)(1)	Receipt/distribution of a visual depiction of a minor engaged in sexually explicit conduct
18 U.S.C. §§ 2252(a)(4)(B) and (b)(2)	Possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct

The application is based on these facts:

See Affidavit of SA Dustin Carder, HSI, attached hereto.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

SA Dustin Carder, HSI

Printed name and title

SWORN AND Attested to by telephone
Sworn to before me and signed in my presence.Date: 6-10-20City and state: Tulsa, OK Tulsa, Oklahoma

Judge's signature

Frank H. McCarthy, U.S. Magistrate

Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT
APPLICATION IN THE NORTHERN DISTRICT OF OKLAHOMA

I, Dustin Carder, being duly sworn under oath, do hereby depose and state:

INTRODUCTION

1. I have been employed as a Special Agent of the United States Department of Homeland Security, Homeland Security Investigations (HSI) in Tulsa, Oklahoma, since December 2018. I am a graduate of the Criminal Investigator Training Program and the Homeland Security Investigations Special Agent Training Academy. As a result of my employment with HSI, my duties include, but are not limited to, the investigation and enforcement of Titles 8, 18, 19, 21, and 31 of the United States Code (U.S.C.). I am an “investigative or law enforcement officer of the United States” within the meaning defined in 18 U.S.C. § 2510(7), in that I am an agent of the United States authorized by law to conduct investigations of, and make arrests for, federal offenses.

2. As part of my duties as an HSI agent, I investigate criminal violations relating to child pornography, including the production, transportation, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, and 2252. I have received training in the areas of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in all forms of media. I have been involved in several child pornography investigations and am familiar with the tactics used by individuals who collect and distribute child pornographic material.

3. This affidavit is made in support of an application for a warrant authorizing the search of the Google account associated with the email address **kayjohns445@gmail.com** (SUBJECT ACCOUNT), that is stored at the premises owned, maintained, controlled, and operated by Google LLC, headquartered at 1600 Amphitheatre Parkway, Mountain View, California, in the Northern District of California. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), to require Google to disclose to the Government records and other information in its possession pertaining to the subscriber(s) or customer(s) associated with the Google account associated with email address **kayjohns445@gmail.com**, including the contents of communications and information more specifically described in Attachment B.

4. The statements included in this affidavit are based in part on an investigation I have conducted, my training and experience, as well as information provided to me by other law enforcement officers, witnesses, and third party sources. As detailed below, I have probable cause to believe that the user(s) of the Google account associated with email address **kayjohns445@gmail.com** has violated federal law, including violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt/distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct) and that evidence relevant to these offenses is currently stored in the Google

account associated with email address **kayjohns445@gmail.com**, more specifically described in Attachment A incorporated with this affidavit.

5. Because this affidavit is being submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me regarding this investigation. I have included only those facts that I believe are necessary to establish probable cause to believe that contraband, evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) are currently stored in the Google records relating to the Google account associated with email address **kayjohns445@gmail.com** (hereinafter, the “**SUBJECT ACCOUNT**”).

6. As disclosed herein, my investigation indicates the **SUBJECT ACCOUNT** was associated with a device synchronized to Google products containing child pornography. Therefore, the facts and circumstances set forth in this affidavit will show probable cause to believe that this Google account will have stored information and communications that are relevant to this investigation.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that - has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(I).

STATUTORY AUTHORITY

8. As noted above, this investigation concerns alleged violations of the following:

- a. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
- b. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

DEFINITIONS

9. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and the attachments incorporated herein:

- a. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct,

(b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

- b. “Internet Protocol address” or “IP address” refers to a unique number used by a computer or electronic device to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.
- c. “Electronic Mail,” commonly referred to as email (or e-mail), is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. Email systems are based on a store-and-forward model; that is, email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need only connect briefly, typically to an email server, for as long a period of time as it takes to send or receive messages. One of the most common methods of obtaining an email account is through a free web-based email service provider such as, Outlook, Yahoo, or Gmail. Anyone with access to the Internet can generally obtain a free web-based email account.
- d. A “hash value” or “hash ID” is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file’s content. A hash value is a file’s “digital fingerprint” or “digital DNA.” Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file’s hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.
- e. “Cloud storage service” refers to a publicly accessible, online storage provider that can be used to store and share files in large volumes. Users of cloud storage services can share links and associated passwords to their stored files with others in order to grant access to their file collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop computers, laptops, mobile phones or tablets, from anywhere. Many services provide free access up to a certain size limit.

- f. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- g. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
- h. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.
- i. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.
- j. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

INFORMATION REGARDING GOOGLE

10. Google LLC is an American multinational technology company specializing in Internet-related services and products. These services and products include online advertising technologies, search functions, cloud computing, and software. Examples of popular Google online services include email (Gmail), cloud storage service (Google Drive), an office suite (Google Docs), a photo sharing and storage service (Google Photos), and a chatting and conferencing service (Hangouts).

11. Gmail is a webmail service that allows account holders to send, receive, and store emails and attached digital files on Google’s servers, or within other Google account

service applications. Such emails and digital files can include photographs, videos, documents, email text, and structured data (i.e., contacts and calendar items). Google subscribers may obtain email accounts with the “gmail.com” domain name. All of Google’s online services are attached to a Gmail address; accordingly, evidence of an offender’s use of a specific Google service to facilitate an offense will include the information and records relating to the associated Gmail account.

12. During the account registration process, Google asks subscribers to provide basic personal information. Based on my training and experience, I am aware that Google stores and maintains electronic communications and information about subscribers of their services, including their email service. This information includes account access information, email transaction information, alternate communication channels, and account application information. This information may constitute evidence of the crimes under investigation as it may contain information that will identify the party in control of the **SUBJECT ACCOUNT**.

13. Google allows account holders to access their files, which are stored on Google’s servers, from any digital device that can access the Google account application’s website (i.e., Internet accessible devices). I submit that evidence directly relating to an offender’s use of Google products to violate federal child exploitation laws may be found in the information maintained on Google’s servers.

FACTS IN SUPPORT OF PROBABLE CAUSE

14. On or about April 1, 2020, I received several CyberTipline Reports from the National Center for Missing and Exploited Children (NCMEC)¹. The Reports were submitted to NCMEC by Google after Google discovered child pornographic images, gifs, and videos had been stored in Google Photos infrastructure and/or Google Drive. The time frame during which Google submitted these reports to NCMEC was between December 3, 2018 and March 30, 2020.

15. Two of the Gmail email accounts responsible for uploading child pornography to Google's infrastructure were kingaling772018@gmail.com and woodsondb77@gmail.com. The investigation revealed that both email accounts were being utilized by the same individual, identified as Daniel Brent Woodson, a registered sex offender in Collinsville, Oklahoma, in the Northern District of Oklahoma. The NCMEC CyberTipline Reports for these accounts showed a total of five (5) files of child pornography uploaded to Google's infrastructure. The files were reviewed by a Google employee and/or a NCMEC analyst prior to my review of the files. I then reviewed the files and based on

¹ The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a private, non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and Child Victim Identification Program. NCMEC makes information submitted to the CyberTipline and Child Victim Identification Program available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC performs its programs of work pursuant to its own private mission and independent business operations. NCMEC does not act in the capacity of or under the direction or control of the government or law enforcement agencies. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.

my training and experience, the files constitute child pornography, as defined in 18 U.S.C. § 2256.

ACQUISITION OF GOOGLE SEARCH WARRANT & ANALYSIS
OF RECORDS AND DATA RETURNED

16. On April 23, 2020, I obtained a federal search warrant in the Northern District of Oklahoma for the Gmail accounts of kingaling772018@gmail.com and woodsondb77@gmail.com. The search warrant was signed by US Magistrate Judge Paul J. Cleary, in the Northern District of Oklahoma, and ordered Google to produce records and content for the accounts. On April 24, 2020, I electronically served Google with the search warrant via Google's Law Enforcement Request System.

17. On April 30, 2020, Google responded to the search warrants for kingaling772018@gmail.com and woodsondb77@gmail.com. After reviewing the information, in woodsondb77@gmail.com's Google Chats folder, I located a chat between woodsondb77@gmail.com and kayjohns445@gmail.com (**SUBJECT ACCOUNT**) in which the **SUBJECT ACCOUNT** received child pornography from woodsondb77@gmail.com. The **SUBJECT ACCOUNT** also shared a link to a cloud storage service with woodsondb77@gmail.com that contained apparent child pornography. The chat log is listed below; I have described the child pornography images that were distributed in the corresponding message blocks. All times listed are Coordinated Universal Time (UTC).

2020-03-19 16:18:08	woodsondb77@gmail.com	Hi... U here? I'm from the chat site
2020-03-19 17:33:03	kayjohns445@gmail.com	Hey
2020-03-19 18:15:24	woodsondb77@gmail.com	Hi .. sorry was feeding my dogs and counting the sheep..
2020-03-19 18:15:57	kayjohns445@gmail.com	Ok
2020-03-19 18:16:14	woodsondb77@gmail.com	[Image posted displaying nude pubescent white female with little breast development, using her hand to partially cover her vagina.]
2020-03-19 18:16:41	woodsondb77@gmail.com	Nice little slut isn't she.... Mmmmm
2020-03-19 18:17:10	woodsondb77@gmail.com	U like all ages?
2020-03-19 18:22:47	kayjohns445@gmail.com	Do you have any links?
2020-03-19 18:22:51	kayjohns445@gmail.com	I have a few
2020-03-19 18:24:00	woodsondb77@gmail.com	Send me them please... And I'll include all pics of these young cock hungry sluts
2020-03-19 18:24:45	woodsondb77@gmail.com	She's 12....
2020-03-19 18:25:02	woodsondb77@gmail.com	;))
2020-03-19 18:45:58	kayjohns445@gmail.com	This is just a little
2020-03-19 18:46:00	kayjohns445@gmail.com	[Link posted to cloud storage service] **Agent note: In an interview, Daniel Woodson described that he observed a video of two girls kissing and engaging in sexual activity after clicking the link. I located this video on Woodson's device and it appears to be two minor females engaging in sexual activity, to include oral sex, with each other. The video is approximately five minutes in length.
2020-03-20 02:48:40	woodsondb77@gmail.com	Ty for that.... Wow! I'd fuck both of those little sluts... Got any more? I do....
2020-03-21 17:27:05	kayjohns445@gmail.com	So do you have more?
2020-03-23 14:30:45	woodsondb77@gmail.com	Yes. Absolutely...
2020-03-23 14:31:09	woodsondb77@gmail.com	Want me to just send?

2020-03-23 14:32:06	woodsondb77@gmail.com	[Image posted of camera looking up dress of prepubescent white female. Female's vagina is displayed in image.]
2020-03-23 14:32:07	woodsondb77@gmail.com	[Image posted that appears to be same female wearing same dress from previous image. Female is seated with legs spread and using fingers to spread apart vagina.]
2020-03-23 14:32:08	woodsondb77@gmail.com	[Image posted that appears again to be same female from previous two images. Female is wearing same dress and is straddling the camera. Female's legs are spread apart, with her vagina and anus visible. Female is using hands to spread apart buttocks to increase visibility of vagina.]
2020-03-23 14:32:51	woodsondb77@gmail.com	And how are you today?? ;-)
2020-03-24 17:56:18	kayjohns445@gmail.com	Send as much as you can since my other links have a lot more
2020-03-28 16:09:27	woodsondb77@gmail.com	Ok. Give me some time.... I'm working today
2020-03-29 03:25:20	woodsondb77@gmail.com	How do I get videos online like you have??
2020-03-29 03:25:49	woodsondb77@gmail.com	[Image posted of different nude prepubescent white female. Female is taking a "selfie" in the mirror with her legs spread fully apart displaying her vagina.]
2020-03-29 03:25:50	woodsondb77@gmail.com	[Image posted of same nude prepubescent white female sitting with legs spread apart, displaying vagina. Female appears to have pen or similar object inserted into her anus.]
2020-03-29 03:25:51	woodsondb77@gmail.com	[Image posted of nude prepubescent white female that appears to be the same female as previous two images. In this image, female is taking another "selfie" in the mirror. Female is positioned on her knees with one hand supporting her and the other hand holding a cellular phone. Female is nearly on all fours but is turned around and taking picture of her vagina displayed in the mirror.]

Based on my training and experience, all of these files described and/or listed above constitute child pornography, as defined in 18 U.S.C. 2256.

18. The aforementioned information indicates the user of the **SUBJECT ACCOUNT** has utilized a Google account, products and services to facilitate the receipt, transportation, distribution, possession, and access with intent to view child pornography. Accordingly, there is probable cause to believe that the search of the **SUBJECT ACCOUNT** will yield contraband, evidence, fruits, and instrumentalities of these crimes.

19. Based on my training and experience in child exploitation investigations, I am aware that Google products including, but not limited to, Gmail, Google Photos, and Google Drive are often used by individuals who receive, transport, distribute and possess child pornography. Child pornography offenders utilize these products to upload, trade, and store child pornography, and to communicate with other individuals regarding the sexual exploitation of children. Indeed, these types of Google services are also preferred by child pornography offenders because they allow offenders to access their collection of child pornography from multiple devices, without having to save content to any specific device. To date, I have been involved in several investigations in which cloud storage accounts or other online platforms were used to distribute, receive, and store images and videos of child pornography.

20. Based on my training and experience, I am also aware that individuals often retain email messages. Individuals involved in the possession, receipt and/or distribution of child pornography often retain email messages related to the sexual exploitation of children for extended periods of time, often for years. Most email accounts, such as those offered by Google, do not automatically delete email messages; therefore, if the user does

not delete the email message, it will remain in the account as long as the account is active. To ensure that the contents of the accounts to be searched remain intact pending the execution of this warrant, a preservation request was sent to Google on or about May 8, 2020, for the information contained in the **SUBJECT ACCOUNT**.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

21. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the Government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, Government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

22. Based on the information set forth in this affidavit, I submit there is probable cause to believe that 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt/distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct) have been violated, and that computer systems under the control of Google LLC will contain contraband, evidence, fruits, and instrumentalities of these crimes. Accordingly, I request that this Court issue a search warrant requiring Google

LLC to produce the records outlined in Attachment A, so that agents may analyze and seize the items outlined in Attachment B.

23. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The Government will execute this warrant by serving it electronically on Google LLC. Because the warrant will be served on Google LLC, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.



Dustin Carder
Special Agent
Homeland Security Investigations

Sworn and Attested to by telephone

Subscribed and sworn to before me on the 10th day of June, 2020.



UNITED STATES MAGISTRATE JUDGE
NORTHERN DISTRICT OF OKLAHOMA

ATTACHMENT A
DESCRIPTION OF ITEMS TO BE SEARCHED

This warrant applies to information associated with the following SUBJECT ACCOUNT: **kayjohns445@gmail.com**, that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, in the Northern District of California.

ATTACHMENT B
DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

In order to ensure that agents search only those computer accounts and/or computer files described herein, this search warrant seeks authorization to permit employees of Google LLC (hereafter, "Google") to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only those accounts and/or computer files described below, the following procedures have been implemented:

- a. The warrant will be presented to Google personnel by law enforcement agents.

Google personnel will be directed to isolate those accounts and files described below;

- b. In order to minimize any disruption of computer service to innocent third parties, the system administrator will create an exact duplicate of the accounts and files associated with **kayjohns445@gmail.com** (SUBJECT ACCOUNT), including an exact duplicate of all information stored in the computer accounts and/or files described below;
- c. Google system administrators will provide the exact duplicate of the accounts and files described below and all information stored in those accounts and/or files to the Special Agent who serves this search warrant;
- d. Google will disclose the responsive data to this search warrant on its electronic Law Enforcement Request System (LERS), according to its policies, to which

the Special Agent who serves this search warrant has access to download and review the files and information.

- e. Law enforcement personnel will thereafter review the information stored in the accounts and files received from Google and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant.

I. Information to be disclosed by Google

To the extent that the information described in Attachment B is within the possession, custody, or control of Google, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs or information that has been deleted but is still available to Google, Google is required to disclose the following information to the Government for each account or identifier associated with **kayjohns445@gmail.com** (SUBJECT ACCOUNT), for the period of Account Creation to March 30, 2020:

- a. The contents of all emails stored in the account, from the time of account creation to present, including stored or preserved copies of emails sent to and from the account, email attachments, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. The contents and records for any and all Google products associated with account identifiers **kayjohns445@gmail.com** (SUBJECT ACCOUNT)

including, but not limited to, Google Drive, Google Hangouts, Gmail, and Google Photos;

- c. Any deleted emails, including any information described in subparagraph “a” above;
- d. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
- f. Any and all Google IDs listed on the subscriber’s Friends list;
- g. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken;
- h. All content and records currently being preserved by Google pursuant to a Preservation Request submitted to this company on or about May 8, 2020;

- i. Google is hereby ordered to disclose the above information to the Government within 14-days of the issuance of this warrant.

II. Information to be seized by the Government

1. All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, messenger logs, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) including, for each account or identifier listed on Attachment A, information pertaining to the following matters, including attempting and conspiring to engage in the following matters:

- a. Any person knowingly transporting, receiving, distributing, accessing with intent to view, or possessing child pornography, as defined at 18 U.S.C. § 2256(8), into, from or between the SUBJECT ACCOUNT;
2. Credit card and other financial information including but not limited to bills and payment records;
3. Evidence of the identity of the individual(s) who used, owned, or controlled the account or identifier listed on Attachment A;
4. Evidence of the times the account or identifier listed on Attachment A was used;
5. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A and other associated accounts.